

IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A broadcast receiving method comprising:

storing first control information in a storage device of a receiver, the first control information containing identification information unique to the receiver and contract information for selecting some of a plurality of different channels, and the first control information required for the receiver to select broadcasted and encrypted contents information, the contract information including a work key encrypted by a master key;

receiving second control information with the receiver via a bi-directional communications channel, the second control information containing contract information for updating;

periodically updating at a first period the contract information of the first control information in the storage device to the contract information contained in the second control information;

sending back a receipt acknowledgement from the receiver via the bi-directional communications channel when the contract information of the first control information is updated;

periodically receiving encrypted ~~first~~ key information which is independent ~~from~~ of the receiver and broadcasted to decrypt the contents information at a second period shorter than the first period, the encrypted key information being encrypted by the work key;

decrypting the encrypted ~~first~~ key information to obtain ~~second~~ decrypted key information;

storing the ~~second~~ decrypted key information in the storage device;

determining whether the stored ~~second~~ decrypted key information is valid based on the contract information; and

decrypting the contents information based on the ~~second~~ decrypted key information that has been determined to be valid.

Claim 2 (Currently Amended): A broadcast receiving method comprising:

storing first control information in a storage device of a receiver, the first control information containing identification information unique to the receiver and contract information for selecting some of a plurality of different channels, and the first control information required for the receiver to select broadcasted and encrypted contents information, the contract information including a work key encrypted by a master key;

receiving second control information with the receiver via a bi-directional communications channel, the second control information containing contract information for updating;

periodically updating at a first period the contract information of the first control information in the storage device to the contract information of the second control information;

sending back a receipt acknowledgement from the receiver via the bi-directional communications channel when the contract information of the first control information is updated;

periodically receiving encrypted ~~first~~ key information which is independent ~~from~~ of the receiver and broadcasted to decrypt the contents information at a second period shorter than the first period, the encrypted key information being encrypted by the work key;

decrypting the encrypted ~~first~~ key information to obtain ~~second~~ decrypted key information;

storing the ~~second~~ decrypted key information in the storage device;

determining whether the stored ~~second~~ decrypted key information is valid based on the contract information; and

decrypting the contents information based on the ~~second~~ decrypted key information that has been determined to be valid and updated contract information of the first control information.

Claim 3 (Currently Amended): A broadcast receiving apparatus communicating with a first distributor which performs bi-directional communications, and a second distributor which performs a broadcast transmission, comprising:

a storage device configured to store first control information containing identification information and contract information, the first control information being required to select encrypted contents information broadcasted by the second distributor, and the contract information including a work key encrypted by a master key;

a first receiver configured to receive second control information distributed by the first distributor via a bi-directional communications channel, the second control information containing contract information for updating;

an update device configured to periodically update at a first period the contract information of the first control information in the storage device to the contract information of the second control information;

a certifying device configured to send back a receipt acknowledgement via the bi-directional communications channel when the contract information of the first control information is updated;

a second receiver configured to periodically receive encrypted ~~first~~ key information broadcasted by the second distributor at a second period shorter than the first period, the ~~first~~ encrypted key information being required to decrypt the contents information, and the encrypted key common to all broadcast receiving apparatuses and encrypted by the work key;

a key decrypting device configured to decrypt the encrypted ~~first~~ key information to obtain ~~second~~ decrypted key information and store the ~~second~~ decrypted key information in the storage device;

a determination device configured to determine whether the stored ~~second~~ decrypted key information is valid based on the contract information; and

a contents decrypting device configured to decrypt the contents information based on the ~~second~~ decrypted key information that has been determined to be valid.

Claim 4 (Original): An apparatus according to claim 3, wherein the first receiver receives the second control information after the broadcast receiving apparatus is certified by the first distributor.

Claim 5 (Original): An apparatus according to claim 3, wherein said first receiver sends a use history required to charge a fee for use of the contents information to the first distributor, and then receives the second control information.

Claim 6 (Currently Amended): A broadcast receiving apparatus communicating with a first distributor which performs bi-directional communications, and a second distributor which performs a broadcast transmission, comprising:

a storage device configured to store first control information containing identification information and contract information, the first control information being including contract information for selecting some of a plurality of different channels, the first control information required to decrypt encrypted contents information broadcasted by the second distributor, and the contract information including a work key encrypted by a master key;

a first receiver configured to receive second control information distributed by the first distributor via a bi-directional communications channel, the second control information containing contract information for updating;

an update device configured to periodically update at a first period the contract information of the first control information in the storage device to the contract information of the second control information;

a certifying device configured to send back a receipt acknowledgement via the bi-directional communications channel when the contract information of the first control information is updated;

a second receiver configured to periodically receive encrypted ~~first~~ key information broadcasted by the second distributor at a second period shorter than the first period, the ~~first~~

encrypted key information being required to decrypt the contents information, ~~and~~ the key information common to all broadcast receiving apparatuses and encrypted by the work key;

a key decrypting device configured to decrypt the encrypted ~~first~~ key information to obtain ~~second~~ decrypted key information and store the ~~second~~ decrypted key information in the storage device;

a determination device configured to determine whether the stored ~~second~~ decrypted key information is valid based on the contract information; and

a contents decrypting device configured to decrypt the contents information based on the ~~second~~ decrypted key information that has been determined to be valid and updated contract information of the first control information.

Claim 7 (Original): An apparatus according to claim 6, wherein the first receiver receives the second control information after the broadcast receiving apparatus is certified by the first distributor.

Claim 8 (Original): An apparatus according to claim 6, wherein the first receiver sends a use history required to charge a fee for use of the contents information to the first distributor, and then receives the second control information.

Claim 9 (Currently Amended): A method of distributing information between a distributor and at least one receiver, comprising:

receiving broadcasted and encrypted contents information with the receiver;

periodically distributing first control information between the receiver and the distributor via a bi-directional communications channel at a first period, the first control information containing contract information for selecting some of a plurality of different channels, which is used to update contract information of second control information stored in the receiver, the contract information including a work key encrypted by a master key, and the second control information containing identification information unique to the receiver

and required for the receiver to periodically decrypt the contents information at a second period shorter than the first period; and

sending back a receipt acknowledgement from the receiver via the bi-directional communications channel when the contract information of the second control information is updated.

Claim 10 (Currently Amended): A method of distributing information between a distributor and at least one receiver, comprising:

receiving broadcasted encrypted contents information with the receiver;

periodically broadcasting first key information and second key information to the receiver from the distributor via a bi-directional communications channel at a first period, the first key information being independent from the receiver and being required for the receiver to decrypt the contents information, ~~and second key information to the receiver from the distributor~~, the second key information being independent from the receiver and required for the receiver to decrypt the contents information and encrypted by the first key information, the contents information being decrypted based on the second key information and decrypt control information containing identification information unique to the receiver and required to periodically decrypt the contents information at a second period shorter than the first period; and

sending back a receipt acknowledgement from the receiver via the bi-directional communications channel when contract information of the decrypt control information is updated.

Claim 11 (Currently Amended): An information distributing apparatus communicating with a receiver, comprising:

a distributor configured to periodically distribute individual control information for updating contract information of decrypt control information to the receiver at a first period, the receiver decrypting the contents information based on decrypt control information

including identification information unique to the receiver and first key information being independent from the receiver and required for the receiver to decrypt second key information, and the second key information being independent from the receiver and required for the receiver to periodically decrypt the contents information at a second period shorter than the first period, the distributor including a subscriber database storing subscriber data including a transmission completion flag configured to be set to a transmission completion state in response to a receipt acknowledgement received from the receiver.

Claim 12 (Original): An apparatus according to claim 11, wherein said distributor certifies the receiver, and then distributes the individual control information.

Claim 13 (Original): An apparatus according to claim 11, wherein said distributor receives a use history required to charge a fee for use of the contents information from the receiver, and then distributes the individual control information.

Claim 14 (Currently Amended): An information distributing apparatus communicating with a receiver, comprising:

a broadcaster configured to periodically broadcast first key information at a first period, the first key information being independent from the receiver and required to decrypt second key information, and the decrypted second key information being independent from the receiver and required to periodically decrypt contents information at a second period shorter than the first period, the receiver receiving broadcasted encrypted contents information, and decrypting the contents information based on decrypt control information and the decrypted second key information, the decrypt information containing individual control information unique to the receiver and required to decrypt the contents information, the broadcaster including a subscriber database storing subscriber data including a transmission completion flag configured to be set to a transmission completion state in response to a receipt acknowledgement received from the receiver.

Claim 15 (Original): An apparatus according to claim 14, wherein said broadcaster certifies the receiver, and then distributes the individual control information.

Claim 16 (Original): An apparatus according to claim 14, wherein said broadcaster receives a use history required to charge a fee for use of the contents information from the receiver, and then distributes the individual control information.

Claim 17 (Currently Amended): A method for distributing information to a receiver comprising:

periodically broadcasting first key information at a first period and encrypted second key information at a second period shorter than the first period to the receiver from a distributor, the first key information being independent from the receiver and required to decrypt the encrypted second key information, and ~~second key information to the receiver from a distributor,~~ the decrypted second key information being independent from the receiver and required to decrypt encrypted contents information, the receiver selecting and decrypting the contents information based on first control information and the decrypted second key information, the first control information containing identification information unique to the receiver and required to select the contents information;

distributing second control information to the receiver via a bi-directional communications channel, the second control information being for updating at least some contents of the first control information in the receiver;

sending back a receipt acknowledgement to the distributor from the receiver via the bi-directional communications channel when the at least some contents of the first control information is updated; and

broadcasting the individual control information if receipt of the individual control information is not confirmed by the receiver.



Claim 18 (Currently Amended): A method for distributing information to a receiver from a distributor, comprising:

periodically broadcasting first key information at a first period and encrypted second key information at a second period shorter than the first period to the receiver from the distributor, the first key information being independent from the receiver and required to decrypt the encrypted second key information, the decrypted second key information being independent from the receiver and required to decrypt encrypted contents information, the receiver decrypting the contents information based on decrypt control information and the decrypted second key information, the decrypt control information containing identification information unique to the receiver and required to select the contents information;

distributing individual control information to the receiver from the distributor via a bi-directional communications channel, the individual control information containing contract information used for updating at least contract information of the decrypt control information stored in the receiver;

sending back a receipt acknowledgement to the distributor from the receiver via the bi-directional communications channel when the contract information of the decrypt control information is updated; and

broadcasting the individual control information when receipt of the individual control information cannot be confirmed by the receiver.

Claim 19 (Canceled).

Claim 20 (Currently Amended): An apparatus distributing information to a receiver comprising:

a first distributor configured to periodically broadcast first key information at a first period and second key information at a second period shorter than the first period, the first key information being independent from the receiver and required to decrypt encrypted second key information, the decrypted second key information being independent from the

receiver and required to decrypt encrypted contents information and to distribute first control information to the receiver via a bi-directional communications channel, the first control information being for updating at least some contents of second control information stored in the receiver, the second control information containing identification information unique to the receiver, the identification information required to decrypt the encrypted contents information; and

a second distributor configured to broadcast the first control information when receipt of the first control information is not confirmed by the receiver as a destination of the individual control information.

Claim 21 (Currently Amended): An information receiving apparatus which communicates with first and second distributors, comprising:

a storage device configured to store first control information required to decrypt broadcasted and encrypted contents information, the first control information containing identification information unique to the receiving apparatus and contract information for selecting some of different channels, the first control information required for the receiving apparatus to select broadcasted and encrypted contents information, the contract information including a work key encrypted by a master key;

a first receiver configured to receive second control information distributed from the first distributor via a bi-directional communication channel, the second control information containing contract information used to update at least contract information of the first control information stored in the storage device or broadcasted by the first distributor;

a transmitter configured to transmit receipt of the information when the first receiver receives the second control information via the bi-directional communications channel;

an update device configured to periodically update at a first period the contract information of the first control information in the storage device to the contract information of the second control information received by the first receiver;

a certifying device configured to send back a receipt acknowledgement via the bi-directional communications channel when the contract information of the first control information is updated;

a second receiver configured to periodically receive encrypted key information broadcasted by the second distributor, the encrypted key information being required to decrypt the encrypted contents information and common to a plurality of broadcast receiving apparatuses at a second period shorter than the first period, the encrypted key information being encrypted by the work key;

a key decrypting device configured to decrypt the encrypted key information to obtain ~~second~~ decrypted key information and store the ~~second~~ decrypted key information in the storage device;

a determination device configured to determine whether the stored ~~second~~ decrypted key information is valid based on the contract information; and

a contents decrypting device configured to decrypt the contents information based on the ~~second~~ decrypted key information that has been determined to be valid.